User Manual: Autonomous Security Auditor Agents

Step-by-Step Guide for IT Professionals and Security Teams

Introduction

This manual provides clear, step-by-step instructions for utilizing Autonomous Security Auditor Agents to enhance your organization's API security posture. It is intended for IT professionals and security teams seeking a streamlined process for policy ingestion, API configuration auditing, and remediation planning. The guide covers the key features and workflows to help you efficiently secure your API infrastructure with minimal manual intervention.

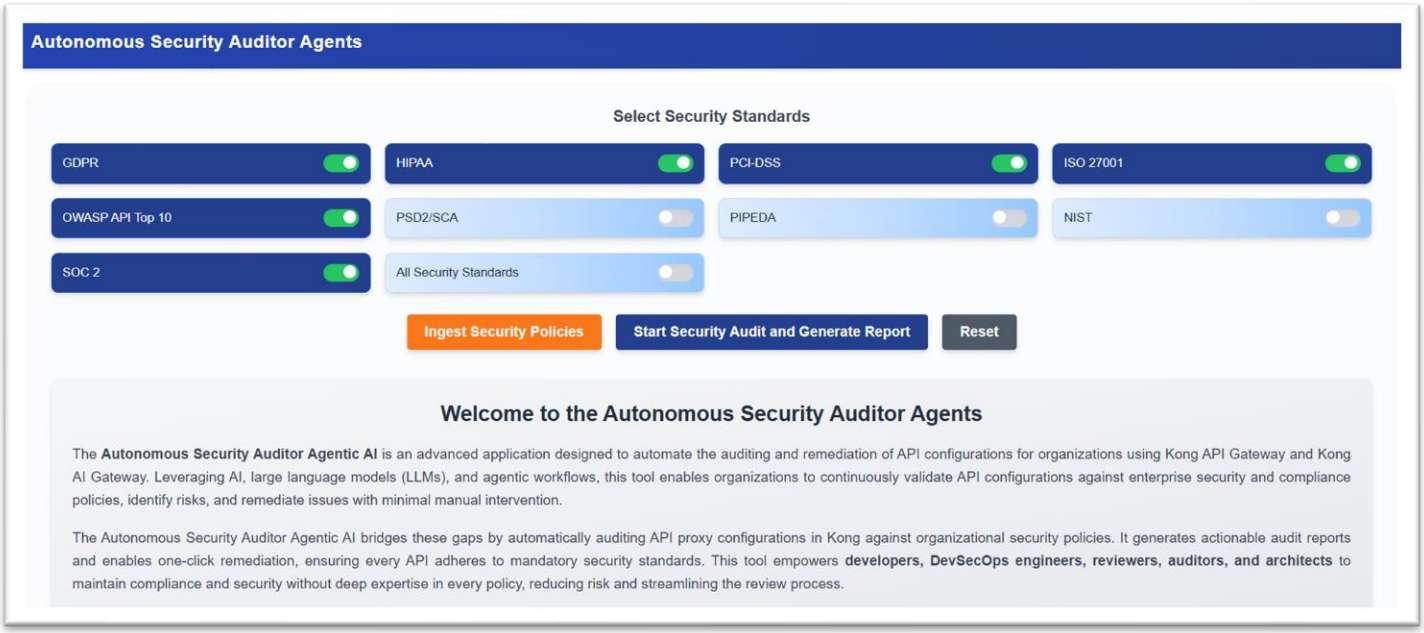
Getting Started

Login Process

To begin using the Autonomous Security Auditor Agents platform, follow these steps:

1. Navigate to the login page of the platform.
2. Enter your assigned credentials (username and password).
3. Click Login to access the home page.

Upon successful login, you will be directed to the Home Page, where you can access all primary features. Refer to the screenshot below for the home page layout:

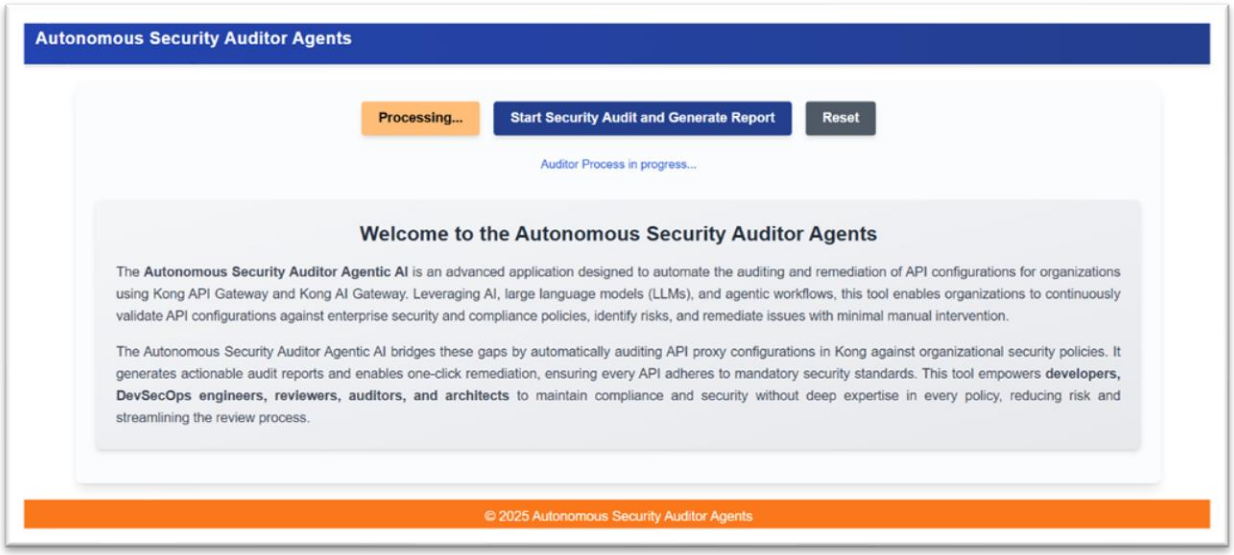


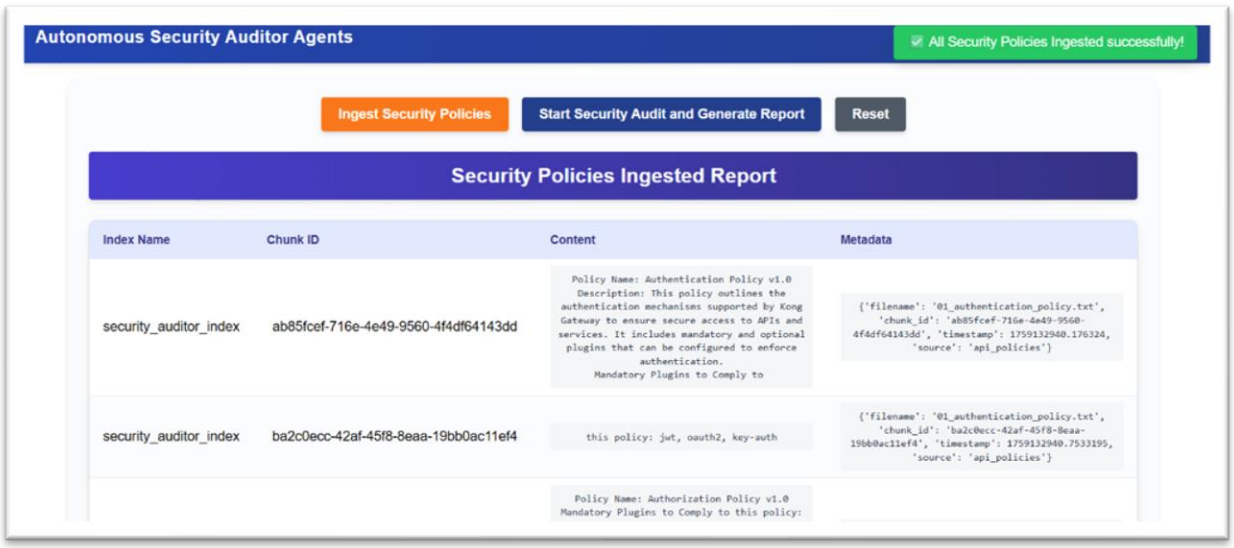
Step 1: Ingesting Organization Security Policies

The first step is to ingest your organization’s security policies into the platform. This allows the system to audit API configurations against established standards.

1. From the Home Page, click on Ingest Policies or the corresponding menu option.
2. Upload your security policy documents by selecting Upload and browsing to the appropriate files.
3. Verify that the policies have been uploaded successfully by checking the confirmation message or reviewing the policy list.

Refer to the screenshot below for the policy ingestion interface:





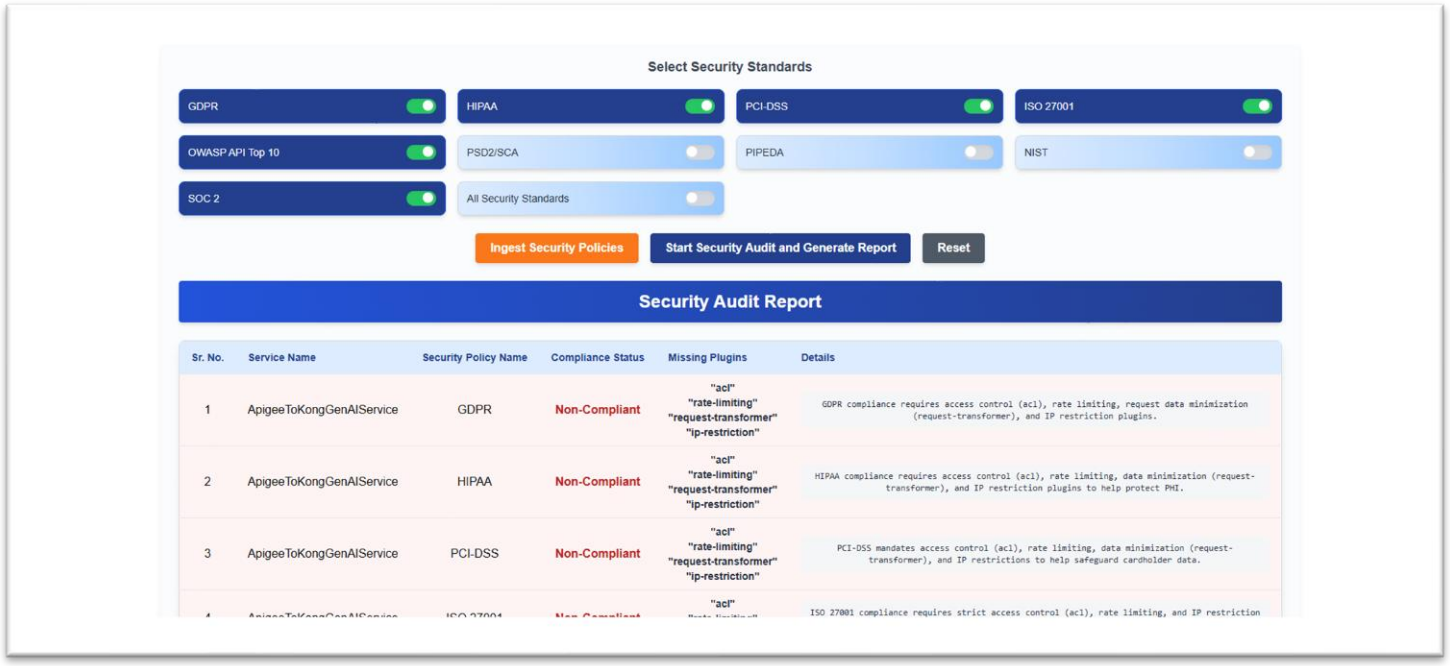
Step 2: Auditing Kong API Configurations

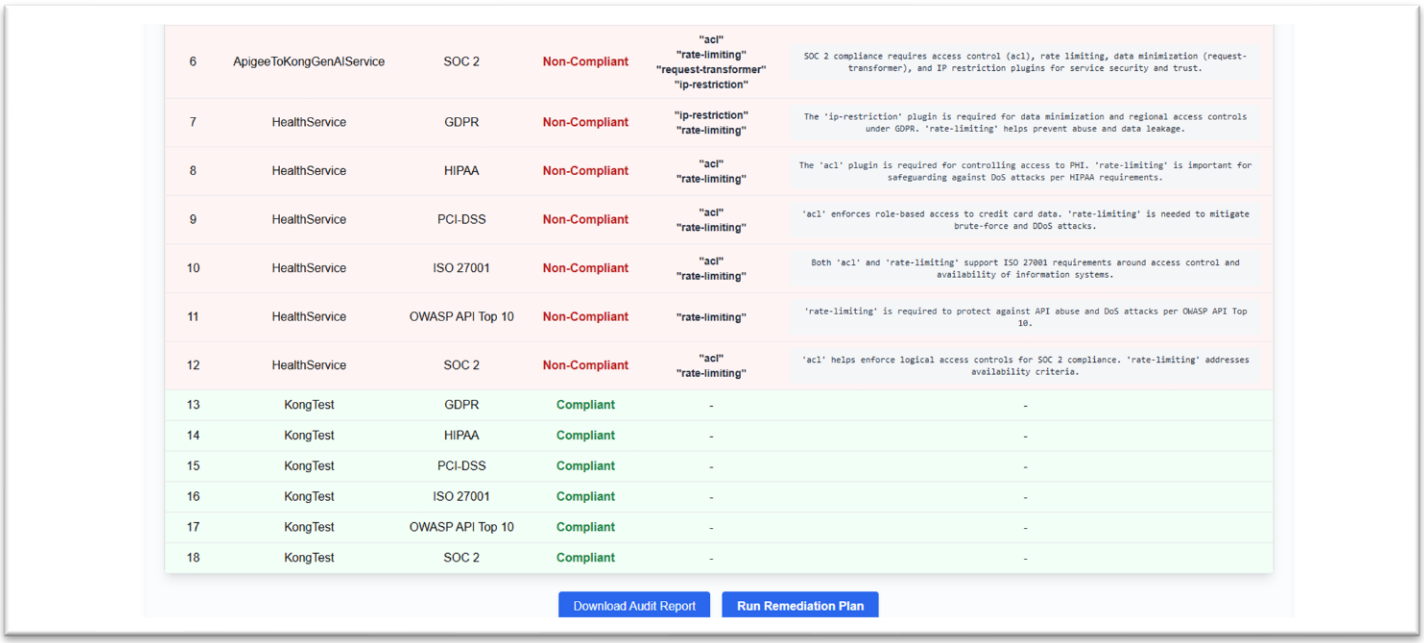
Using the Audit AI Agent

With your security policies in place, the Audit AI Agent can now assess your Kong API configurations for compliance.

1. Navigate to the Audit section on the Home Page.
1. Choose the security standards you wish to audit for Kong API proxies.
2. Click Start Audit to initiate the automated analysis.
3. Monitor the progress via the on-screen status indicators.
4. Once complete, review the generated audit report for findings and recommendations.

Screenshots below illustrate the audit initiation and report review process:





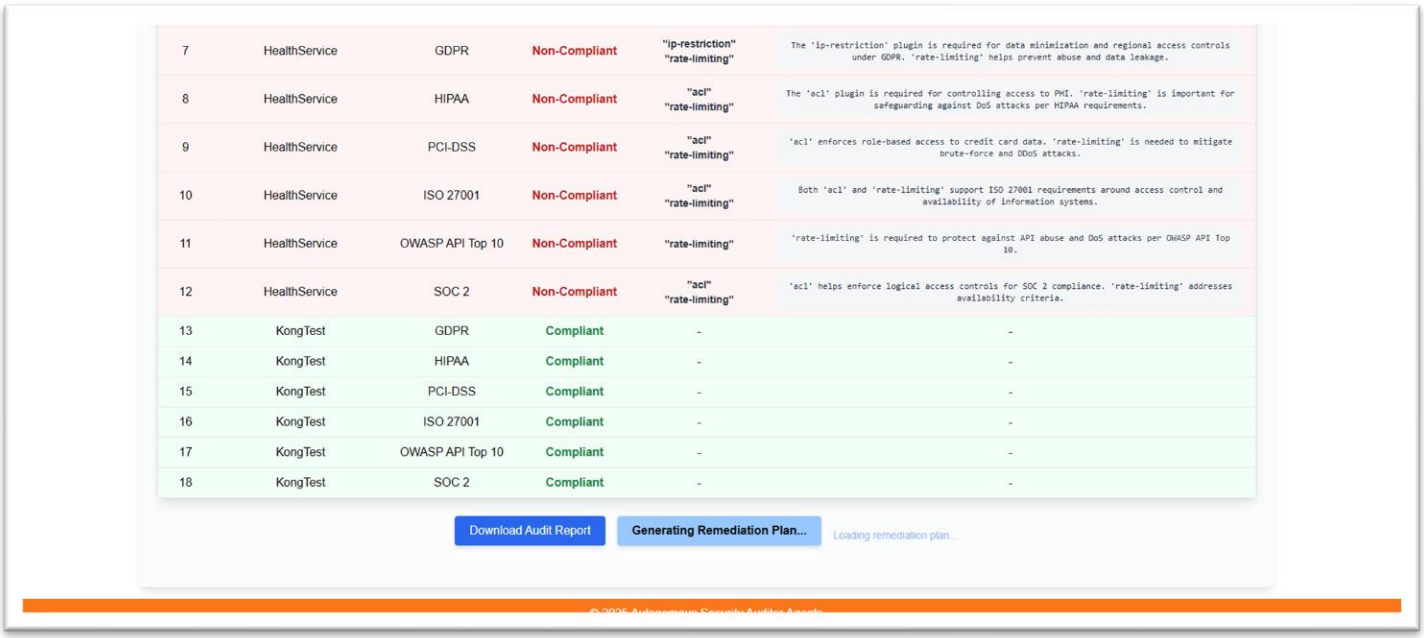
Step 3: Remediating Audit Reports and Generating Remediation Plans

Using the Remediate Agent

After reviewing the audit findings, you can use the Remediate Agent to create and implement a remediation plan.

1. From the audit report, click on Run Remediation Plan button.
2. The Remediate Agent will generate a detailed remediation plan based on the identified issues.
3. Review the proposed actions and modify them as needed to fit your environment.
4. Approve and apply the remediation plan by clicking Apply Plan.
5. Monitor the status of remediation and confirm completion via the dashboard.

See below for screenshots demonstrating the remediation workflow:



Remediation Plan

Service Name	Policy Name	Issue	Missing Plugin(s)	Recommended Action	Severity	Owner	Estimated Effort
ApigeeToKongGenAIService	GDPR	Missing mandatory plugins for GDPR compliance.	acl, rate-limiting, request-transformer, ip-restriction	Enable the 'acl', 'rate-limiting', 'request-transformer', and 'ip-restriction' plugins to meet GDPR requirements for access control, rate limiting, data minimization, and IP restriction.	Medium	API Security Team	4h
ApigeeToKongGenAIService	HIPAA	Missing mandatory plugins for HIPAA compliance.	acl, rate-limiting, request-transformer, ip-restriction	Enable the 'acl', 'rate-limiting', 'request-transformer', and 'ip-restriction' plugins to ensure proper access control, traffic management, data minimization, and restricted IP access for PHI protection.	Medium	API Security Team	4h
ApigeeToKongGenAIService	PCI-DSS	Missing mandatory plugins for PCI-DSS compliance.	acl, rate-limiting, request-transformer, ip-restriction	Enable 'acl', 'rate-limiting', 'request-transformer', and 'ip-restriction' plugins to enforce access control, prevent abuse, minimize sensitive data exposure, and restrict IPs per PCI-DSS requirements.	Medium	API Security Team	4h

Remediation Plan

Issue	Missing Plugin(s)	Recommended Action	Severity	Owner	Estimated Effort	Impact	Security Standard Reference
Missing mandatory plugins for GDPR compliance.	acl, rate-limiting, request-transformer, ip-restriction	Enable the 'acl', 'rate-limiting', 'request-transformer', and 'ip-restriction' plugins to meet GDPR requirements for access control, rate limiting, data minimization, and IP restriction.	Medium	API Security Team	4h	High; failing GDPR compliance exposes the organization to regulatory penalties and privacy breaches.	GDPR
Missing mandatory plugins for HIPAA compliance.	acl, rate-limiting, request-transformer, ip-restriction	Enable the 'acl', 'rate-limiting', 'request-transformer', and 'ip-restriction' plugins to ensure proper access control, traffic management, data minimization, and restricted IP access for PHI protection.	Medium	API Security Team	4h	High; non-compliance may lead to unauthorized access or exposure of protected health information.	HIPAA
Missing mandatory plugins for PCI-DSS compliance.	acl, rate-limiting, request-transformer, ip-restriction	Enable 'acl', 'rate-limiting', 'request-transformer', and 'ip-restriction' plugins to enforce access control, prevent abuse, minimize sensitive data exposure, and restrict IPs per PCI-DSS requirements.	Medium	API Security Team	4h	High; risk of breaches involving cardholder data and regulatory fines.	PCI-DSS

		compliance.					
HealthService	HIPAA	Missing mandatory plugins for HIPAA compliance.	acl, rate-limiting	Enable 'acl' and 'rate-limiting' plugins to enforce access restrictions and protect against traffic abuse.	Medium	API Security Team	2h
HealthService	PCI-DSS	Missing plugins required for PCI-DSS compliance.	acl, rate-limiting	Enable 'acl' for role-based access and 'rate-limiting' to protect payment data integrity.	Medium	API Security Team	2h
HealthService	ISO 27001	Missing plugins required for ISO 27001 compliance.	acl, rate-limiting	Enable 'acl' and 'rate-limiting' plugins to align with access control and availability measures.	Medium	API Security Team	2h
HealthService	OWASP API Top 10	Missing plugin required for OWASP API Top 10 protection.	rate-limiting	Enable the 'rate-limiting' plugin to guard against API abuse and DoS attacks.	Medium	API Security Team	1h
HealthService	SOC 2	Missing plugins required for SOC 2 compliance.	acl, rate-limiting	Enable 'acl' to support logical access and 'rate-limiting' to ensure availability.	Medium	API Security Team	2h

			compliance.					
	Missing mandatory plugins for HIPAA compliance.	acl, rate-limiting	Enable 'acl' and 'rate-limiting' plugins to enforce access restrictions and protect against traffic abuse.	Medium	API Security Team	2h	High; PHI may be improperly accessed or exposed.	HIPAA
	Missing plugins required for PCI-DSS compliance.	acl, rate-limiting	Enable 'acl' for role-based access and 'rate-limiting' to protect payment data integrity.	Medium	API Security Team	2h	High; failure to control access or usage jeopardizes cardholder data and may incur penalties.	PCI-DSS
	Missing plugins required for ISO 27001 compliance.	acl, rate-limiting	Enable 'acl' and 'rate-limiting' plugins to align with access control and availability measures.	Medium	API Security Team	2h	Medium; missing controls undermine ISMS objectives.	ISO 27001
0	Missing plugin required for OWASP API Top 10 protection.	rate-limiting	Enable the 'rate-limiting' plugin to guard against API abuse and DoS attacks.	Medium	API Security Team	1h	Medium; API may be vulnerable to excessive requests.	OWASP
	Missing plugins required for SOC 2 compliance.	acl, rate-limiting	Enable 'acl' to support logical access and 'rate-limiting' to ensure availability.	Medium	API Security Team	2h	High; missing controls could affect audit outcomes and service reliability.	SOC 2

Conclusion

By following these steps, your organization can leverage Autonomous Security Auditor Agents to efficiently ingest security policies, audit API configurations, and implement remediation plans. For additional assistance or resources, please contact Sachin Ghumbre.